Doc Code: AP.PRE.REQ

PTO/SB/33 (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): GFP108US

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on February 15, 2010

Signature /Leslie Ann Menges/

Typed or printed name Leslie Ann Menges

Application Number	Filed
10/816,661	April 2, 2004

First Named Inventor: Marufa Kaniz, et al.

Art Unit	Examiner
2434	Yonas A. Bayou

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 36981.
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/Thomas G. Eschweiler/
Signature

Thomas G. Eschweiler
Typed or printed name

(216) 502-0600
Telephone number

February 15, 2010
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

Docket No. GFP108US H1246

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re **PATENT** application of:

Applicant:	Marufa Kaniz et al
Application No.:	10/816,661
For:	METHODS AND APPARATUS FOR PASSING INITIALIZATION VECTOR INFORMATION FROM SOFTWARE TO HARDWARE TO PERFORM IPSEC ENCRYPTION OPERATION
Filing Date:	April 02, 2004
Examiner:	Bayou, Yonas A
Art Unit:	2434

PRE-APPEAL BRIEF IN RESPONSE TO ADVISORY ACTION DATED JANUARY 26, 2010

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Favorable reconsideration of the above-identified application is respectfully requested in view of the following amendments and remarks.

REMARKS

Claims 1-6, 8-12, and 14-23 are pending. Reconsideration of the application in light of the following remarks is respectfully requested.

I. REJECTION OF CLAIMS 1-6, 8-12, and 14-23 UNDER 35 U.S.C. § 103(a)

Claims 1-6, 8-12, and 14-23 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. US 7,003,118 B1 Yang et al. (Yang) in view of U.S. Patent No. US 6,418,130 B1 Cheng et al. (Cheng). Withdrawal of the rejection is respectfully requested for at least the following reasons.

i. The cited art does not teach a security system that is adapted to employ an initial random data string from outgoing data to begin encryption, as recited in claim 1.

Claim 1 recites a network interface system, comprising a security system adapted to employ an ***initial random data string*** from outgoing data to begin encryption before security association information has been retrieved by the security system. Claim 15 recites a method of encrypting outgoing data in a network interface system comprising selectively employing an initialization vector, comprising an ***initial random data string*** from outgoing data. The Office Action concedes that Yang does not teach such a security system, but instead alleges that Cheng teaches a security system adapted to employ an initial random data string. (*See, O.A. of 11/16/09*, p. 6, lns. 4-10). However, as will be more fully appreciated below, Chang fails to teach a security system adapted to employ an ***initial random data string*** from outgoing data to begin encryption, as recited in claims 1 and 15.

More particularly, Cheng teaches a wireless communication system configured to reuse, rather than renegotiate, security associations (SAs). The Advisory Action of 1/26/10 notes, as illustrated in Fig. 4 where SA attributes are transferred from SU_k to SU_{k+1}, that the transferred SA attributes include transferring a last IKE phase 1 CBC output block prior to hand over, which is used as the initialization vector for encryption of the first IP packet subsequent to hand over. (*See*, *Cheng*, col. 6, lns. 61-63). In other words, an IKE phase 1 CBC block, calculated for SU_k is transferred to SU_{k+1} to be used as an initialization vector, so that an initialization vector does not have to be recalculated.

Accordingly, Cheng teaches a method of "***reusing previously established security associations*** [between MU and SU_k] to support newly formed connections between the MU (mobile unit) and SU_{k+1}" to avoid renegotiating SAs each time an MU changes its point of connection." (*See*, Col. 3, lns. 53-61). However, the term "***re-using***" means that the SAs were ***previously negotiated***. Since a previously negotiated SA is not ***an initial random data string***, Cheng does not teach an initial

random data string, as recited in claims 1 and 15. Accordingly, for at least this reason, applicant respectfully requests withdrawal of the rejection of claims 1 and 15, and the claims which depend therefrom.

ii. The cited art does not teach a security system that is adapted to employ an initial random data string from outgoing data to begin encryption, as recited in claims 1 and 15.

Claim 1 recites a network interface system, comprising a security system adapted to employ an initial random data string from outgoing data to begin encryption before security association information has been retrieved by the security system. Claim 15 recites a method of encrypting outgoing data in a network interface system comprising selectively employing an initialization vector (IV), comprising an initial random data string from outgoing data. The Office Action concedes that Yang does not teach such a security system, but instead alleges that Cheng teaches a security system adapted to employ an initial random data string from outgoing data. (*See, O.A. of 11/16/09*, p. 6, lns. 4-10). However, as will be more fully appreciated below, Cheng fails to teach a security system adapted to employ ***an initial random data string from outgoing data***, as recited in claims 1 and 15.

As stated above, Cheng teaches a wireless communication system configured to reuse security associations (SAs). In particular, Cheng notes that SU_k, upon receiving a request from SU_{k+1}, sends a reply message containing information necessary to define the ISAKMP SA attribute (comprising CBC output block). (*See*, col. 6, lns. 45-63). Therefore, the CBC output block (associated with claimed initialization vector) ***is part of the reply message sent from SU_{k+1} to SU_k***. However, the reply vector is only relayed between SU_k and SU_{k+1} and ***does not comprise outgoing data***. Because the reply vector does not comprise outgoing data, the CBC block (initialization vector), as taught by Cheng, is not a data string ***from outgoing data***, as recited in claims 1 and 15, but rather is only from a reply message sent between stationary units. Accordingly,

for at least this additional reason, applicant respectfully requests withdrawal of the rejection of claims 1 and 15, and the claims which depend therefrom.

iii. The cited art fails to teach a security system adapted to employ an initial random data string from outgoing data to begin encryption before security association information has been retrieved by a security system, as recited in claims 1 and 15.

Claim 1 recites a network interface system comprising a security system adapted to employ an initial random data string from outgoing data to begin encryption before security association information has been retrieved by the security system. Claim 15 recites a method for encrypting outgoing data in a network interface system comprising encrypting outgoing data before security association information has been retrieved by the security system. The Office Action concedes that Yang does not teach this limitation, but instead alleges that Cheng teaches "the security system is adapted to employ an initial random data string from the outgoing data ***to begin encryption before security association information has been retrieved*** by the security system." (*See, O.A. of 11/16/09*, p. 4, par. 5 – p. 5 par. 1). However, as will be more fully appreciated below, Cheng does not teach this limitation of claims 1 and 15.

Cheng describes in par. 1:48-60 that ISAKMP SAs are negotiated in Phase 1 before negotiating IPsec SAs and subsequent encryption in Phase 2. That is, the two phases are ***not independent***. Thus, Cheng teaches that a negotiated SA takes place in both phases 1 and 2 ***before encryption in phase 2***. (*See, e.g.*, col. 7, lns. 7-11; stating "the first time a MU connects to any SU in a given administrative domain, an IKE phase 1 negotiation and an IKE phase 2 negotiation must be accomplished, thereby establishing the ISAKMP SA and the IP_{SEC} SAs respectively."). Therefore, Cheng does not teach employing an initial random data string from the outgoing data to begin encryption ***before SA information has been retrieved*** by the security system.

Further, Cheng relies upon ***reusing previously established security associations*** to support these newly formed connections between MU and SU_{k+1}.

However, in order to ***re-use*** **an SA**, Cheng ***must first have previously negotiated*** the SA, which can then be re-used in a subsequent hand-over.

By contrast, the claimed security system is adapted to begin encryption ***before*** security association information has been retrieved. Since, the claimed security system begins encryption before retrieving an SA, in contrast to the teaching of Cheng which first establishes an SA before it can be "re-used" to begin encryption in an IPsec phase II, Cheng fails to teach over the claimed invention.

Accordingly, for at least this additional reason, applicant respectfully requests withdrawal of the rejection of claims 1 and 15, and the claims which depend therefrom.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, GFP108US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600